A case study in almost-perfect security for unconditionally secure communication

Esteban Landerreche*

David Fernández-Duque†

Instituto Tecnológico Autónomo de México
Río Hondo 1, 01080 Mexico City, Mexico

June 23, 2015

Abstract

In the Russian cards problem, Alice, Bob and Cath draw a, b and c cards, respectively, from a publicly known deck. Alice and Bob must then communicate their cards to each other without Cath learning who holds a single card. Solutions in the literature provide *weak security,* where Alice and Bob's exchanges do not allow Cath to know with certainty who holds each card that is not hers, or *perfect security,* where Cath learns no probabilistic information about who holds any given card. We propose an intermediate notion, which we call ε-strong security, where the probabilities perceived by Cath may only change by a factor of ε. We then show that a mild variant of the so-called *geometric strategy* gives ε-strong safety for arbitrarily small ε and appropriately chosen values of a, b, c.

1 Introduction

Consider the following problem, which appeared in the 2000 Moscow Mathematics Olympiad:

> Alice, Bob and Cath draw three, three and one cards, respectively, from a publicly known deck of seven. Alice and Bob wish to inform each other of the cards they hold, but they may only do so by public, unencrypted announcements. Moreover, they do not wish for Cath to know who holds a single card that is not hers. Can Alice and Bob achieve this?

---

*`estebanlan@gmail.com`
†`david.fernandez@itam.mx`

It later came to be known as the *Russian cards problem* [13], and is interesting from a cryptographical viewpoint since it provides a framework for *unconditionally secure communication,* perhaps the strongest notion of security that one may demand from a cryptographic protocol.

1.1 Notions of cryptographic security

Claude Shannon, one of the first people to formalize the study of cryptography, proposed several notions of *cryptographic security.* To be precise, he defined the following:

- **Computational Security**: We say that a protocol is **computationally secure** for n if at least n operations are needed to break it. It is usually very difficult to prove that protocol is secure in this sense, as we would need to know all the possible strategies for attack. However, it is a good measure of when a system *isn't* secure, that is, when it fails to be secure for a relatively small n.

- **Provable Security**: We say that a protocol is **provably secure** if we can link it with a 'hard' problem, cryptographic or not, in such a way that solving the second problem will allow us to break the encryption. In that case, we know that we need at least as many operations to break the code as we need to solve the second problem. Typically, the 'hard' problem is in NP but believed to not be in P. Many of the cryptographic protocols in use today are based on this notion of security.

- **Unconditional Security**: A protocol is **unconditionally secure** if it can't be broken even with unlimited computational resources; the eavesdropper simply does not have enough information to reconstruct the original message.

It should be clear that unconditional security implies both computational and provable security, and as such it would ideally be desirable to develop unconditionally secure cryptographic protocols. However, such protocols tend to be unpractical and as such few of them are known, with a notable example being Vernam's one time pad [10]. However, the setup of the Russian cards, which presupposes a secure dealing phase, provides a convenient setup for developing unconditionally secure protocols.

1.2 Related work

The Russian cards problem may be traced back to Kirkman [8], but recently it has received renewed attention after its inclusion in the 2000 Mathematics Olympiad [13]. One of the solutions for deals of distribution type $(3, 3, 1)$ uses the Fano plane, a special case of a combinatorial design, which can also be used for many other distribution types [1]. Another solution uses modular arithmetic,

which can also be generalized for many distribution types where the eavesdropper holds one card [3]. These solutions use only two announcements, but some cases are known to require more. A solution using three announcements for $(4, 4, 2)$ is reported in [14], and a four-step protocol for $c = O(a^2)$ and $b = O(c^2)$ is presented in [4]. The solution we will work with in this paper is similar to the one reported in [2], which also takes two steps. The Russian cards problem has also been generalized to a larger number of agents in [6, 7].

However, while the protocols mentioned above provide unconditionally secure solutions to the Russian cards problem in that the eavesdropper may not *know with certainty* who holds a given card, that does not mean that she may not have a high probability of *guessing* this information correctly. To this end, stronger notions of security are studied in [12]. There, a distinction is made between *weak* and *perfect* security; in perfectly secure solutions, Cath does not acquire any probabilistic information about the ownership of any specific card. All of the above solutions provide weak security in this sense, but Swanson and Stinson show how designs may be used to achieve perfect security, an idea further developed in [11].

The solutions we present here will provide an intermediate level of security between weak and perfect, controlling the amount of probabilistic information that may be acquired by the eavesdropper, while having the advantage of being much easier to construct than perfectly secure solutions.

2   A Worked Example

We will motivate the work in this article with a relatively small example. Let's suppose we have 49 cards, with Alice holding 7, Cath holding 5 and Bob the rest. In this case, Alice can take advantage of the fact that there is a field $\mathbb{F}_7$ with 7 elements (the quotient $\mathbb{Z}/(7)$ forms a field), and thus may identify each point in the two-dimensional vector space over $\mathbb{F}_7$, which we will denote $\mathbb{F}_7^2$, with a card. Moreover, she can do this in such a way that her cards (marked by ♠) form a line. Suppose then that Cath holds the cards marked by ♣, while Bob holds the rest of the cards (♢).

Alice then announces how she has distributed the cards on the plane. In this particular announcement, Cath's cards all fall within the same line. This is an extreme case, but it is a real possibility, as Alice has no knowledge of Cath's hand when she makes her announcement. Bob and Cath know that Alice's hand falls on a line, but they do not know which line. Bob then knows exactly which cards Alice holds (since there is only one complete line that he does not hold), but Cath does not. However, she may consider it more likely that Alice holds one card over another. To illustrate this, let us consider the points labeled x and y in Figure 2.

First we will take a look at x. Cath knows that, in order for Alice to hold x, one of the lines that passes through x must be Alice's hand. We draw these lines on the plane.

Cath knows that not all the lines that pass through x can be Alice's hand,
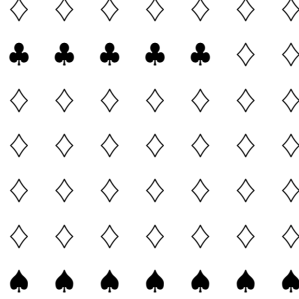
Figure 1: Alice assigns each card to a point on the plane in such a way that her hand forms a line. She does not know how the other cards will fall, since she can only see her own hand. In this example, all of Cathy's cards happen to fall on another line.

because if a line contains a card that belongs to Cath, it clearly cannot be held in its entirety by Alice . In this case, only one line fits that description, so Cath takes it out of consideration. We denote this by drawing the line dotted. Every point in the plane has 8 lines that cross it; therefore, the point x still belongs to 7 hands that could possibly belong to Alice.

However, this is not the case for all cards that Cath does not hold. Let us now turn our attention to y. While x was colinear with Cath's hand, all the lines that contain y and one of Cath's cards are different. In this case Cath can discard more lines than she could when considering x. Only 3 possible lines remain, compared to the 7 lines that pass through x and avoid Cath's hand. Therefore, it seems to Cath that the point x would be more likely to belong to Alice's hand than the point y as there are more possible hands that contain it. Before the announcement, both cards had the same probability to be in Alice's hand but after the announcement, x seems far more likely.

Note that the total number on lines in the announcement is 56. We also know that 36 of these lines contain a card that Cath holds. This is because there are 8 lines touching each point, but the 5 points all share one line. Therefore Alice's hand is one of the 20 lines that avoid Cath's hand. Of those 20 only three contain y compared to the 7 that contain x. Thus, it seems to Cath that there is a $7/20 = 0.35$ probability that Alice holds x compared to $3/20 = 0.15$ that she holds y. Thus, according to the information that Cath has, it is more than twice as likely that Alice holds x as it is that she holds y.

In this case, we know neither of the cards actually belongs to Alice, but we want to be able to quantify this information and control it, especially in higher dimensions where it is not as simple to visualize. Our goal is to show that, by choosing different parameters appropriately, we can make the different probabilities be arbitrarily close to each other. But first we need some preliminaries to make this precise.
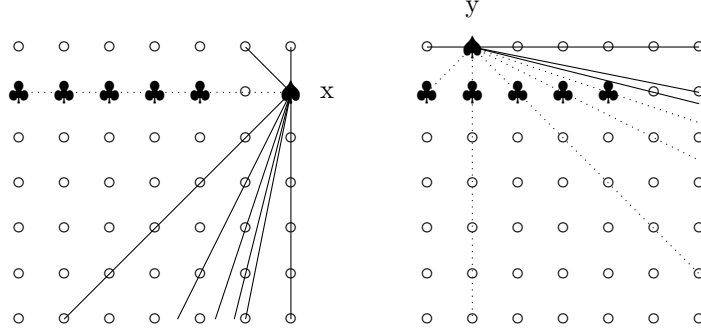
4

Figure 2: Lines that Cath may discard from Alice's announcement. It is important to note that most of the lines are truncated, as the natural representation of $\mathbb{F}_7^2$ is as a torus and lines are harder to visualize in two dimensions.

3 Strategies and Probabilistic Security

In this section we will set up the basic concepts needed to formalize the Russian cards problem and different notions of security that one may require from its possible solutions. We will assume that Alice holds a cards, Bob b and Cath c, and Ω is the set of cards with $|\Omega| = a + b + c$. A **deal (of size** (a, b, c)**)** is a partition (A, B, C) of Ω such that $|A| = a$, $|B| = b$ and $|C| = c$; each of A, B, C represent the hand of Alice, Bob and Cath, respectively.

3.1 Equitable strategies

In most solutions to the Russian cards problem, Alice makes an announcement, after which Bob knows the entire deal and thus can make a second (trivial) announcement where he tells Alice which cards Cath holds. Thus we need only model Alice's first announcement, and we follow [12] in referring to the way that Alice is to choose her announcement as a *strategy*.

Suppose that Alice holds a cards, Bob holds b and Cath holds c. Given a set X and a natural number n, we denote by $\binom{X}{n}$ the set of n-element subsets of X, and we will refer to such sets as *n-sets*. We denote the cardinality of X by $|X|$. A possible hand for Alice is then an element of $\binom{\Omega}{a}$. In Alice's first announcement she gives a set of possible hands that she may hold, and thus we may consider an announcement simply as a set $\mathcal{A} \subset \binom{\Omega}{a}$.

However, there are many possible announcements that may inform Bob of Alice's hand, and it may be convenient for Alice to randomize from all such possible announcements. Thus a strategy for Alice consists on a probability distribution among the possible announcements that she may choose from.

Definition 1. *A **strategy (on** $\binom{\Omega}{a}$**)** is a function $\mathfrak{S}$ that assigns to each hand $A \in \binom{\Omega}{a}$ a probability distribution over $2^{\binom{\Omega}{a}}$. We denote the probability of an*

5

announcement $\mathcal{A}$ given the hand A as $P_{\mathfrak{S}}(\mathcal{A}|A)$.

Given a strategy $\mathfrak{S}$ and a hand A, we will say that $\mathcal{A}$ is a possible announcement if $P_{\mathfrak{S}}(\mathcal{A}|A) > 0$. The set of possible announcements will be denoted by $\mathfrak{S}_A$.

When it is clear from context, we will drop the subindex $\mathfrak{S}$ and write simply $P(\mathcal{A}|A)$ to simplify notation. It will also be convenient for computations if the number of possible announcements is independent of Alice's hand. If we could guarantee that there are m possible announcements for each hand, we could always assign a probability of $1/m$ to each individual announcement. If a strategy has this property, we will say it is equitable [12].

Definition 2. *A strategy $\mathfrak{S}$ is **equitable** if there exists a positive integer m such that, for every a-set A, $|\mathfrak{S}_A| = m$ and the probability of choosing a particular announcement $\mathcal{A} \in \mathfrak{S}_A$ is $P(\mathcal{A}|A) = 1/m$.*

One advantage of equitable strategies is that we need less information to specify them than more general strategies. In particular, we may model equitable strategies merely as a function

$$\mathfrak{S} \colon \binom{\Omega}{a} \to 2^{2^{\binom{\Omega}{a}}},$$

where $\mathfrak{S}_A$ is the set of announcements with positive probability (and thus with probability $1/m$). Since the geometric strategy, which will be our main focus, is equitable, we will adopt this presentation.

The first condition that a two-step solution to the Russian cards problem should satisfy is that Bob should be informed of Alice's hand after an announcement. Let us make this precise. First, we introduce an abuse of notation that we will use throughout the text.

If $\mathcal{X} \subset 2^{\Omega}$ and $Y \subset \Omega$, define

$$\mathcal{X} \setminus Y = \{X \in \mathcal{X} : X \cap Y = \varnothing\}.$$

Thus, $\mathcal{X} \setminus Y$ is the set of elements of $\mathcal{X}$ avoiding Y.

Definition 3. *Fix integers a, b, c and a deck Ω with $|\Omega| = a+b+c$. A strategy $\mathfrak{S}$ on $\binom{\Omega}{a}$ is **informative for** (a, b, c) if, for every $A \in \binom{\Omega}{a}$ and every $B \in \binom{\Omega \setminus A}{b}$, $\mathfrak{S}_A \setminus B = \{A\}$.*

Thus after an informative announcement, Bob knows exactly which hand A Alice is holding. But an informative strategy may also give Cath information, yet we also require for Alice's strategy to be secure.

3.2 Probabilistic Security

Before Alice makes an announcement, Cath knows that Alice can possibly hold any hand that doesn't contain one of Cath's cards. Hence, there are $\binom{a+b}{a}$ possible hands for Alice. However, after an announcement, Cath can discard

any hand that isn't found in the announcement. After doing so, it is possible that Cath acquires new information about the cards she does not hold. In particular, she may know that there is a high probability that Alice holds a given card. If Alice and Bob want to communicate securely, it would be desirable to avoid giving Cath such information.

There are three different notions of probabilistic security for strategies: weak, perfect, and our notion of ε-strong security, which lies between the other two. Unconditional security is equivalent to weak security. If we wanted to avoid Cath learning any probabilistic information after an announcement, we would need to ensure that no card seems more likely after the announcement than it did before. For this, the number of hands in the announcement (after Cath eliminates the ones which have a card that she holds) that contain a given card must be equal for every card that Cath does not hold. In this case, the probability of Alice having a set card should stay the same after Alice's announcement. As a matter of fact, we know the value of this probability; we must only count the hands that could contain that card given Cath's hand and divide it by the number of remaining hands in the announcement:

$$P(x \in A|C) = \frac{\binom{a+b-1}{a-1}}{\binom{a+b}{a}} = \frac{a}{a+b}.$$

If this number stays constant after Alice's announcement, we will say that Alice's strategy is perfectly secure.

Definition 4. *A strategy* $\mathfrak{S}$ *on* $\binom{\Omega}{a}$ *is **perfectly secure for** (a, b, c) *if for every* $C \in \binom{\Omega}{c}$, *every card* $x \in \Omega \setminus C$, *and every announcement* $\mathcal{A}$ *with* $P(\mathcal{A}|C) \neq 0$, *we have that*

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} = 1.$$

This notion is equivalent to 1-perfect security in [12] and represents Cath's inability to gleam information about the position of individual cards. Compare this to *weak security,* where we only require that Cath is not certain about the position of any card she does not hold.

Definition 5. *A strategy* $\mathfrak{S}$ *on* $\binom{\Omega}{a}$ *is **weakly secure for** (a, b, c) *if for every* $C \in \binom{\Omega}{c}$, *every card* $x \in \Omega \setminus C$, *and every announcement* $\mathcal{A}$ *with* $P(\mathcal{A}|C) \neq 0$, *we have that*

$$0 < \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} < 1.$$

In [11, 12], the authors present examples of perfectly secure strategies when Cath has at most 3 cards. Due to the rigidity needed to ensure this level of security, it is not clear whether perfectly secure strategies can be constructed when Cath holds more cards. Instead, we will define an intermediate level of security, where the constraint is relaxed so we can have more flexibilty and can work in cases where Cath's hand is larger. In fact, this notion will permit us to find secure protocols for any possible hand size that Cath may hold.

Definition 6. *Let $\varepsilon > 0$. A strategy $\mathfrak{S}$ on $\binom{\Omega}{a}$ is ε-**strongly secure for** (a, b, c) if for every $C \in \binom{\Omega}{c}$, every card $x \in \Omega \setminus C$, and every announcement $\mathcal{A}$ with $P(\mathcal{A}|C) \neq 0$, we have that*

$$\left| \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} - 1 \right| < \varepsilon.$$

As mentioned above, equitable strategies are useful for simplifying computations. In particular, the above probabilities may be computed by counting. The following result can be found in [12].

Lemma 1. *Let $\mathfrak{S}$ be an equitable strategy on $\binom{\Omega}{a}$ and (A, B, C) be a deal. Suppose that $C \in \binom{\Omega}{c}$ and $\mathcal{A}$ is an announcement with $P(\mathcal{A}|C) > 0$ and $A \in \mathcal{A}$. Then, $P(A|C, \mathcal{A}) = \frac{1}{|\mathcal{A} \setminus C|}$.*

In other words, the probability that A is Alice's hand given Cath's hand C and the announcement $\mathcal{A}$ (when A is a valid hand given C) is given by the quotient of one over the number of hands in the announcement that avoid C.

Thus the probability of Alice having a set hand A according to Cath is $1/|\mathcal{A} \setminus C|$. However, what we want to calculate is the probability that Alice holds a given card x. For this, we introduce a new abuse of notation: for $\mathcal{X} \subseteq 2^{\Omega}$ and $y \in \Omega$, set

$$\mathcal{X}_y = \{X \in \mathcal{X} : y \in X\}.$$

Thus for $Z \subset \Omega$, $\mathcal{X}_y \setminus Z$ denotes the set of elements of $\mathcal{X}$ which contain y but avoid Z. The following can also be found in [12].

Lemma 2. *Let $\mathfrak{S}$ be an equitable strategy on $\binom{\Omega}{a}$ and (A, B, C) be a deal. If $z \in \Omega \setminus C$, then*

$$P(z \in A|C, \mathcal{A}) = \frac{|\mathcal{A}_z \setminus C|}{|\mathcal{A} \setminus C|}.$$

4 Finite geometries

The geometric strategy is convenient because it allows us to use many familiar results from linear algebra. One key difference when working over finite fields (instead of, say, $\mathbb{R}$) is that now it becomes relevant to count the number of points in a subspace, the number of subspaces touching a point, etc. These quantities will be useful more than once in this article.

First, we recall a general result about the cardinalities of finite fields. Results in this section are presented without proof; for a more thorough treatment of finite fields and finite geometry, the reader may consult a text such as [5, 9].

Theorem 1 (Existence and Uniqueness of Finite Fields)**.** *If q is a natural number, there exists a finite field with cardinality q if and only if q is of the form p^n, with p a prime and n a positive integer. This field is unique up to isomorphism and is called the **Galois Field of order** q. We will denote it by $\mathbb{F}_q$.*

Our protocol will be based on affine subspaces of a finite vector space. For brevity, we will refer to an affine space of dimension α as an 'α-plane', while an α-plane passing through the origin (i.e., a linear subspace of dimension α) will be referred to as an 'α-space'.

Definition 7. *Let $\mathbb{V}$ be a vector space over a field $\mathbb{F}$. We say that $W \subset \mathbb{V}$ is an α-**space** if it is a an α-dimensional subspace of $\mathbb{V}$.*

*A subset $U \subseteq \mathbb{V}$ is an α-**plane** if it is of the form $x + W$, where $x \in \mathbb{V}$ and W is an α-space. Two α-planes X, Y are **parallel** if there exists $y \in \mathbb{V}$ such that $Y = y + X$.*

Thus an α-plane is similar to an α-space, although it does not necessarily pass through the origin. If $\mathbb{F}$ is finite, then it is not difficult to count the number of points on an α-plane.

Lemma 3. *If q is a prime power and $\mathbb{V}$ is a vector space over $\mathbb{F}_q$, then any α-plane in $\mathbb{V}$ has exactly q^α points.*

Meanwhile, the intersection of two distinct α-planes is either empty or a η-plane for some $\eta < \alpha$, which has the following consequence.

Lemma 4. *If q is a prime power, $\mathbb{V}$ is a vector space over $\mathbb{F}_q$ and $U, W \subseteq \mathbb{V}$ are distinct α-planes, then*

1. $|U \cap W| \leq q^{\alpha-1}$ *and*

2. $|U \cup V| \geq 2q^\alpha - q^{\alpha-1}$.

We may also fix a point x in our vector space and instead ask how many α-planes meet x. Here the dimension of $\mathbb{V}$ will be relevant. We will denote the δ-dimensional vector space over $\mathbb{F}_q$ by $\mathbb{F}_q^\delta$.

Definition 8. *Fix a prime power q. Then, given positive integers $\alpha \leq \delta$, define*

$$[\dot{\alpha}]_{q,\delta} = \prod_{i=1}^{\alpha} \left(\frac{q^\delta - q^{i-1}}{q^\alpha - q^{i-1}} \right).$$

Lemma 5. *Let q be a prime power and $\delta \geq \alpha > 0$. Then,*

1. *Given $x \in \mathbb{F}_q^\delta$, the total number of α-planes meeting x is equal to $[\dot{\alpha}]_{q,\delta}$.*

2. *Given distinct points $x, y \in \mathbb{F}_q^\delta$, the number of α-planes meeting both x and y is given by*
$$[\ddot{\alpha}]_{q,\delta} = \left(\frac{q^\alpha - 1}{q^\delta - 1} \right) [\dot{\alpha}]_{q,\delta}.$$

3. *The total number of α-planes in $\mathbb{F}_q^\delta$ is $q^{\delta-\alpha} [\dot{\alpha}]_{q,\delta}$.*

9

Proof. For the first claim, we may assume without loss that $x = 0$. Fix q and let k_α^δ denote the number of (ordered) sequences $v_1, \ldots, v_\alpha$ of linearly independent vectors in $\mathbb{F}_\alpha^\delta$. Observe that, for each α-space W, there are exactly k_α^α ordered bases for W, and thus the total number of α-spaces is precisely $k_\alpha^\delta / k_\alpha^\alpha$.

Thus it suffices to find an expression for k_α^δ. For v_1, we have $q^\delta - 1$ options, since we may choose any vector in $\mathbb{F}_q^\delta$ save for 0. For v_2, we have $q^\delta - q$ options, since we may choose any vector that does not lie in the line generated by v_1. More generally, for v_i we have $q^\delta - q^{i-1}$ options, since we may choose any vector that does not lie in the $(i-1)$ space generated by $v_1, \ldots, v_{i-1}$. Thus the total number of options is

$$k_\alpha^\delta = \prod_{i=1}^{\alpha} (q^\delta - q^{i-1}),$$

and hence the total number of α-spaces is

$$\frac{k_\alpha^\delta}{k_\alpha^\alpha} = \frac{\prod_{i=1}^{\alpha}(q^\delta - q^{i-1})}{\prod_{i=1}^{\alpha}(q^\alpha - q^{i-1})} = [\dot{\alpha}]_{q,\delta}.$$

The second claim is proven in a similar fashion. As before, we may assume that $x = 0$ and fix $y \neq 0$. Then we proceed as above, except that we fix v_1 to be y. This removes the first factor from both the numerator and the denominator, giving us

$$[\ddot{\alpha}]_{q,\delta} = \frac{\prod_{i=2}^{\alpha}(q^\delta - q^{i-1})}{\prod_{i=2}^{\alpha}(q^\alpha - q^{i-1})} = \left(\frac{q^\alpha - 1}{q^\delta - 1} \right) [\dot{\alpha}]_{q,\delta}.$$

Finally, for the third claim, note that if we fix an α-space W, the α-planes parallel to W, together with W, form a partition of $\mathbb{F}_q^\delta$, hence there are $q^\delta / q^\alpha = q^{\delta - \alpha}$ of them. But there are $[\dot{\alpha}]_{q,\delta}$ different α-spaces, and thus the total number of α-planes is $q^{\delta - \alpha}[\dot{\alpha}]_{q,\delta}$. $\qquad \square$

5   The Geometric Strategy

We've informally presented the geometric solution to the Russian Cards problem, and will now formalize it to construct the Geometric Strategy. The protocol we will use is essentially presented in [2]. The basic idea is to construct a finite vector space where every point represents a different card and Alice's hand forms an α-plane. Below, we use $f[X]$ to denote the set $\{f(x) : x \in X\}$. Each announcement is parametrized by a *suitable map*.

Definition 9. *Fix a prime power q, natural numbers $0 < \alpha < \delta$ and $A \in \binom{\Omega}{a}$. We define a* suitable map *for A to be a function $f : \Omega \to \mathbb{F}_q^\delta$ such that $f[A]$ is an α-plane.*

Given a suitable map f, we define

$$\mathcal{A}[f] = \{X \subset \Omega : f[X] \text{ is an } \alpha\text{-plane}\}.$$

The geometric strategy is then defined by letting Alice choose uniformly from all suitable maps f and announcing $\mathcal{A}[f]$.

Definition 10 (The geometric strategy)**.** *Let q be a prime power and $0 < \alpha < \delta$. Given a, b and c such that $a = q^\alpha$ and $a + b + c = q^\delta$, we define the **geometric strategy (with parameters** q, α, δ**)**, denoted $\mathfrak{G} = \mathfrak{G}(q, \delta, \alpha)$, to be the strategy such that $\mathfrak{G}_A$ is the set of all announcements of the form $\mathcal{A}[f]$, where $f \colon \Omega \to \mathbb{F}_q^\delta$ is suitable for A, and Alice chooses uniformly from $\mathfrak{G}_A$.*

This strategy generalizes that in [2] where $\alpha = \delta - 1$, although that article also considers the case where Alice holds more than one plane. Let us now show that the strategy is equitable.

Lemma 6. *Let q be a prime power, $0 < \alpha < \delta$ and $a = q^\alpha$, and let $\mathfrak{G} = \mathfrak{G}(q, \delta, \alpha)$. Then, if $A, A' \in \binom{\Omega}{a}$, $|\mathfrak{G}_A| = |\mathfrak{G}_{A'}|$.*

Proof. Let $A, A' \in \binom{\Omega}{a}$. To show that $|\mathfrak{G}_A| = |\mathfrak{G}_{A'}|$, we will define a bijection $\Sigma \colon \mathfrak{G}_A \to \mathfrak{G}_{A'}$. As a first step, we will build a function σ that permutes the elements of Ω. We know that $|A \setminus A'| = |A' \setminus A|$, so we can find a bijection $s \colon A \setminus A' \to A' \setminus A$.

Using the function s we will define a permutation $\sigma \colon \Omega \to \Omega$ given by

$$
\sigma(x) = \begin{cases} s(x) & \text{if } x \in A \setminus A' \\ s^{-1}(x) & \text{if } x \in A' \setminus A \\ x & \text{otherwise.} \end{cases}
$$

Since s is invertible, σ is well-defined, and it is easy to check that σ is bijective. We then define $\Sigma \colon \mathfrak{G}_A \to \mathfrak{G}_{A'}$ given by $\Sigma(\mathcal{A}) = \{\sigma[H] | H \in \mathcal{A}\}$. Then, it is easy to see that Σ has an inverse given by $\Sigma^{-1}(\mathcal{B}) = \{\sigma^{-1}[H] : H \in \mathcal{B}\}$, and hence Σ is a bijection, so that $|\mathfrak{G}_A| = |\mathfrak{G}_{A'}|$ as claimed. $\square$

We have now proven that for every hand that Alice can have there is the same number m of possible announcements. This permits us to set the probability of a particular announcement to be chosen to $1/m$, and thus the geometric strategy is equitable. As mentioned above, this will simplify some computations, even without explicitly computing m.

In the remainder of this section we will prove that the geometric strategy gives an informative and weakly safe solution to the Russian cards problem, provided c satisfies certain bounds.

Lemma 7. *Let q be a prime power, $1 \le \alpha < \delta$ and a, b, c positive integers such that $a = q^\alpha$, $a + b + c = q^\delta$ and $c < q^\alpha - q^{\alpha-1}$. Then, the geometric strategy with parameters q, δ, α is informative for (a, b, c).*

Proof. Let $q, \delta, \alpha, a, b, c$ satisfy the hypotheses of the lemma. Let $A \in \binom{\Omega}{a}$ and $B \in \binom{\Omega \setminus A}{b}$ and $f \colon \Omega \to \mathbb{F}_q^\delta$ be such that $f[A]$ is an α-space. Clearly $A \in \mathfrak{G}_A$, so it remains to check that if $A' \in \binom{\Omega \setminus B}{a}$ is such that $\mathcal{A}[f] \in \mathfrak{G}_{A'}$, then $A = A'$.

If this were not the case, then $U = f[A]$ would be an α-space different from $U' = f[A']$. Since both U and U' are disjoint from $f[B]$, then so is $U \cup U'$. By Lemma 4.2, $|U \cup U'| \ge 2q^\alpha - q^{\alpha-1}$. But f is a bijection, so it follows that

11

$a + c = |A| + |C| \geq 2q^\alpha - q^{\alpha-1}$, and thus $c \geq q^\alpha - q^{\alpha-1}$, contradicting our hypothesis.

We conclude that $U = U'$, so that also $A = A'$ and thus the geometric strategy is informative. $\square$

Next we must see that, given a card x not held by Cath, there is a nonzero probability that Alice holds x, which means that it is impossible that there is $x \in \Omega \setminus C$ such that all α-spaces passing through x meet C.

Lemma 8. *Let q be a prime power, $0 < \alpha \leq \delta$ and a, b, c be such that $a = q^\alpha$ and $a + b + c = q^\delta$. Let $C \in \binom{\Omega}{c}$, and $f \colon \Omega \to \mathbb{F}_q^\delta$ be a bijection. If $c < \frac{q^\delta - 1}{q^\alpha - 1}$ and $x \in \Omega \setminus C$, there is $A \in \mathcal{A}[f]$ such that $x \in A$.*

Proof. Let $x \in \Omega \setminus C$. Recall that $[\dot\alpha]_{q,\delta}$ is the number of α-planes meeting $f(x)$. If we take $z \in C$, there are $[\ddot\alpha]_{q,\delta}$ α-planes touching both x and z and, since there are c points in C, there are at most $c[\ddot\alpha]_{q,\delta}$ α-planes touching $f(x)$ and meeting $f[C]$. Thus in order to guarantee that there is at least one α-plane touching $f(x)$ but not $f[C]$, it suffices to have $c[\ddot\alpha]_{q,\delta} < [\dot\alpha]_{q,\delta}$. Solving for c and using Lemma 5.2, this becomes

$$c < \frac{[\dot\alpha]_{q,\delta}}{[\ddot\alpha]_{q,\delta}} = \frac{q^\delta - 1}{q^\alpha - 1}.$$

Thus if c satisfies this constraint, there is an α-space U touching $f(x)$ but not meeting $f[C]$ and $A = f^{-1}[U]$ is an element of $\mathcal{A}[f]$ containing x but disjoint from C, as desired. $\square$

Likewise, there should be a nonzero probability that any card not held by Cath is held by Bob. In other words, if y is not held by Cath, there should be an α-plane avoiding y *and* Cath's hand.

Lemma 9. *Let q be a prime power, $0 < \alpha \leq \delta$ and a, b, c be such that $a = q^\alpha$ and $a + b + c = q^\delta$. Let $C \in \binom{\Omega}{c}$ and $f \colon \Omega \to \mathbb{F}_q^\delta$ be a bijection. If $c < q^{\delta-\alpha}$ and $y \in \Omega \setminus C$, there is $A \in \mathcal{A}[f]$ such that $y \notin A$ and $A \cap C = \varnothing$.*

Proof. Let $y \in \Omega \setminus C$ and $z \in C$ be arbitrary and V be an α-plane touching both $f(y)$ and $f(z)$. We know that there are $q^{\delta-\alpha}$ α-planes parallel or equal to V. Thus if $c < q^{\delta-\alpha}$ there is at least one α-plane U parallel to V which does not contain any pont from C. But by construction, y is not on U either. Thus there is an α-plane avoiding both y and U, and we may take $A = f^{-1}[U]$. $\square$

Lemma 10. *Let q be a prime power, $0 < \alpha < \delta$ and a, b, c be such that $a = q^\alpha$ and $a + b + c = q^\delta$. Then, the geometric strategy with parameters q, α, δ is weakly secure for (a, b, c) whenever $c < q^{\delta-\alpha}$.*

Proof. It is straightforward to check that $q^{\delta-\alpha} < \frac{q^\delta - 1}{q^\alpha - 1}$, so this is a direct consequence of Lemmas 8 and 9. $\square$

Putting together Lemmas 7 and 10 we obtain the main result of this section.

Theorem 2. *Let q be a prime power, $0 < \alpha < \delta$ and a, b, c be such that $a = q^\alpha$ and $a + b + c = q^\delta$. Then, the geometric strategy with parameters q, α, δ is weakly safe and informative for (a, b, c) whenever $c < \min(q^\alpha - q^{\alpha-1}, q^{\delta-\alpha})$.*

We may use Theorem 2 to find many tuples (a, b, c) for which the geometric strategy is weakly secure. If Alice holds a line in the plane, then we may take c to be almost as large as a:

Corollary 1. *There are infinitely many values of a such that for any $c \leq a - 2$ there is $b < a^2$ such that the geometric strategy is informative and weakly safe for (a, b, c).*

Proof. Take $\alpha = 1$, $\delta = 2$ and q an arbitrary prime power and apply Theorem 2. □

On the other hand, if c is much smaller, then we can give Alice a higher-dimensional plane to ensure that the number of cards is not too large relative to Alice and Cath's hands.

Corollary 2. *Given rational $\rho \in (0, 1)$, there are infinitely many values of a such that for any $c < a^\rho$ there is $b < a^{1+\rho}$ such that the geometric strategy is informative and weakly safe for (a, b, c).*

Proof. Since ρ is rational, so is $1 + \rho$, so we can find $1 \leq \alpha < \delta$ such that $1 + \rho = \delta/\alpha$. Since $\rho < 1$, for large enough q we have that $q^{\rho\alpha} < q^\alpha - q^{\alpha-1}$. Thus for such a q we may use Theorem 2 to see that, for $a = q^\alpha$, $c < q^{\delta-\alpha}$ and $b = q^\delta - a - c$, the geometric strategy is informative and weakly safe. Moreover, we have that $b < q^\delta = q^{(1+\rho)\alpha} = a^{(1+\rho)}$, whereas $c < q^{\delta-\alpha} = q^{\rho\alpha} = \alpha^\rho$ was arbitrary, so all desired conditions are met. □

Observe that in either case, the geometric strategy gives infinitely many solutions for tuples (a, b, c) with $c < a$ and $b < ac$.

6 Strong safety of the geometric strategy

Since the geometric strategy is equitable, we may apply the results in the previous section to it in order to find parameters for which this strategy is ε-strongly safe. As we have seen, this strategy is weakly safe if $c < q^\alpha - q^{\alpha-1}$ and $c < q^{\delta-\alpha}$. Our goal will be to find tuples for which it is ε-strongly safe for a given ε.

6.1 Some auxiliary estimates

We will need to find bounds on the number of hands that Cath considers possible. We begin by counting the total number of hands in an announcement. The following is a direct consequence of Lemma 5.

Lemma 11. *The number of a-sets in an announcement $\mathcal{A}$ of the geometric strategy with parameters q, δ, α is $q^{\delta-\alpha} [\dot{\alpha}]_{q,\delta}$.*

Now let us see how many hands Cath can discard from this announcement. Recall that $\mathcal{A} \setminus C$ denotes the set of lines avoiding C and $\mathcal{A}_x \setminus C$ denotes the set of lines avoiding C that also pass through x. We may compute the probability that Alice holds x from Cath's perspective as

$$P(x \in A | C, \mathcal{A}) = \frac{|\mathcal{A}_x \setminus C|}{|\mathcal{A} \setminus C|}.$$

What we are interested in is bounding the quotient of Cath's perceived probabilites before and after the announcement, that is,

$$\frac{P(x \in A | C, \mathcal{A})}{P(x \in A | C)} = \frac{|\mathcal{A}_x \setminus C| / |\mathcal{A} \setminus C|}{a / a + b}. \tag{1}$$

As we will see, by modifying the parameters, this quotient can become arbitrarily close to 1.

In order to find bounds for (1), it suffices to bound the numerator, since the denominator is constant. Thus we need to estimate $|\mathcal{A}_x \setminus C|$ and $|\mathcal{A} \setminus C|$. Let us begin with the latter.

Lemma 12. *If $\mathcal{A}$ is an announcement of the geometric strategy with parameters α, δ, q and $C \in \binom{\Omega}{c}$ is non-empty, then*

$$[\dot{\alpha}]_{q,\delta}(q^{\delta - \alpha} - c) \leq |\mathcal{A} \setminus C| \leq [\dot{\alpha}]_{q,\delta}(q^{\delta - \alpha} - 1). \tag{2}$$

Both equalities hold whenever $c = 1$.

Proof. By Lemma 11, $|\mathcal{A}| = q^{\delta - \alpha} [\dot{\alpha}]_{q,\delta}$. Thus we may estimate the number of α-planes that meet C and subtract to obtain our bounds.

Suppose that $\mathcal{A} = \mathcal{A}[f]$. To bound $|\mathcal{A} \setminus C|$ from below, observe that there are $[\dot{\alpha}]_{q,\delta}$ α-planes passing through each point in $f[C]$ and there are c such points, so that the number of hands in $\mathcal{A}$ meeting C, which is equal to the number of α-planes touching $f[C]$, is at most $c[\dot{\alpha}]_{q,\delta}$. It follows that

$$[\dot{\alpha}]_{q,\delta}(q^{\delta - \alpha} - c) \leq |\mathcal{A} \setminus C|.$$

Observe that when $c > 1$ we are subtracting one α-plane at least twice so the inequality is strict, but when $c = 1$ then equality holds.

Now let us show the right-hand inequality. Since $C \neq \varnothing$, we can pick $z \in C$ and observe that there are $[\dot{\alpha}]_{q,\delta}$ α-planes meeting $f(z)$, and thus *at least* $[\dot{\alpha}]_{q,\delta}$ meeting $f[C]$. It follows that

$$|\mathcal{A} \setminus C| \leq [\dot{\alpha}]_{q,\delta} q^{\delta - \alpha} - [\dot{\alpha}]_{q,\delta} = [\dot{\alpha}]_{q,\delta}(q^{\delta - \alpha} - 1),$$

and if $C = \{z\}$ this computation is exact. $\square$

Lemma 13. *If $\mathcal{A}$ is an announcement of the geometric strategy with parameters α, δ, q and $C \in \binom{\Omega}{c}$ is non-empty, then*

$$[\dot{\alpha}]_{q,\delta} - c[\ddot{\alpha}]_{q,\delta} \leq |\mathcal{A}_x \setminus C| \leq [\dot{\alpha}]_{q,\delta} - [\ddot{\alpha}]_{q,\delta}. \tag{3}$$

Equality holds when $c = 1$.

Proof. Once again suppose that $\mathcal{A} = \mathcal{A}[f]$. First let us bound $|\mathcal{A}_x \setminus C|$ from below. To give our estimate, we will take the number of α-planes passing through $f(x)$ and subtract the number of α-planes passing through $f(x)$ and $f(y)$ for each $y \in C$, *without* taking into account that many α-planes will be subtracted twice. Evidently this bound will not be tight, but it will be sufficient to establish our main results.

Recall that $[\dot{\alpha}]_{q,\delta}$ counts *all* of the α-planes passing through a given point. But, there are $[\ddot{\alpha}]_{q,\delta}$ α-planes passing through $f(x)$ and $f(y)$ for each $y \in C$, and thus there are at most $c[\ddot{\alpha}]_{q,\delta}$ planes meeting both $f(x)$ and $f[C]$, hence also hands in $\mathcal{A}$ meeting x and C. It follows that

$$[\dot{\alpha}]_{q,\delta} - c[\ddot{\alpha}]_{q,\delta} \le |\mathcal{A}_x \setminus C|.$$

Now let us bound $|\mathcal{A}_x \setminus C|$ from above. This time we use the fact that there is at least one $y_0 \in C$, and we can discard all of those α-planes that touch $f(y_0)$ as well as $f(x)$, of which there are $[\ddot{\alpha}]_{q,\delta}$. It follows that

$$|\mathcal{A}_x \setminus C| \le [\dot{\alpha}]_{q,\delta} - [\ddot{\alpha}]_{q,\delta},$$

and the result follows. Once again this bound is exact when $c = 1$. $\qquad\square$

6.2 Bounding probabilities

The counting lemmas we have given above may be used to bound the probabilities we are interested in. First, we give a more exact bound, and later we will give a simplified version.

Lemma 14. *If $\mathcal{A}$ is an announcement of the geometric strategy with parameters q, α, δ and $C \in \binom{\Omega}{c}$ is non-empty,*

$$\frac{q^{2\delta} - cq^{\delta+\alpha} - q^{\delta} + c^2(q^{\alpha} - 1) + c}{q^{2\delta} - q^{\delta} - q^{\delta+\alpha} + q^{\alpha}} \le \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} \tag{4}$$

and

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} \le \frac{q^{2\delta} - cq^{\delta} - q^{\delta+\alpha} + cq^{\alpha}}{q^{2\delta} - cq^{\delta+\alpha} - q^{\delta} + cq^{\alpha}}. \tag{5}$$

Proof. For the lower bound, we put the lower bound of Lemma 13 together with the upper bound of Lemma 12 to obtain

$$\frac{[\dot{\alpha}]_{q,\delta} - [\ddot{\alpha}]_{q,\delta}c}{[\dot{\alpha}]_{q,\delta}(q^{\delta-\alpha} - 1)} \le \frac{|\mathcal{A}_x \setminus C|}{|\mathcal{A} \setminus C|} = P(x \in A|C, \mathcal{A}).$$

Using Lemma 5.2 and simplifying we obtain

$$\frac{q^{\delta} - cq^{\alpha} + c - 1}{q^{2\delta-\alpha} - q^{\delta-\alpha} - q^{\delta} + 1} \le P(x \in A|C, \mathcal{A}).$$

15

a	b	c	q	α	δ	Lower	Upper
23	504	2	23	1	2	0.9547	1.0456
43	1,803	3	43	1	2	0.9524	1.0488
64	4,028	4	2^6	1	2	0.9524	1.0492
529	11,636	2	23	2	3	0.9545	1.0475
1,849	77,655	3	43	2	3	0.9523	1.0499
4,096	258,044	4	2^6	2	3	0.9523	1.0499
12,167	267,672	2	23	3	4	0.9545	1.0476
79,507	3,339,291	3	43	3	4	0.9523	1.0499
262,144	16,515,068	4	2^6	3	4	0.9523	1.0499

Figure 3: Some choices of parameters for the geometric strategy along with their respective lower and upper bounds given by Lemma 14. These were found by fixing $c \in \{2, 3, 4\}$, $\alpha \leq 3$ and $\delta = \alpha + 1$ and finding the least q for which the strategy is 0.05-strongly safe.

Thus,

$$\frac{\frac{q^\delta - cq^\alpha + c - 1}{q^{2\delta - \alpha} - q^{\delta - \alpha} - q^\delta + 1}}{\frac{a}{a+b}} \leq \frac{P(x \in A | C, \mathcal{A})}{P(x \in A | C)};$$

using the equalities $a = q^\alpha$ and $a + b + c = q^\delta$ and simplifying once again we obtain

$$\frac{q^{2\delta} - cq^{\delta + \alpha} - q^\delta + c^2(q^\alpha - 1) + c}{q^{2\delta} - q^\delta - q^{\delta + \alpha} + q^\alpha} \leq \frac{P(x \in A | C, \mathcal{A})}{P(x \in A | C)}.$$

Now we turn to bounding the quotient of probabilities from above. As before, we focus on the numerator, since the denominator is fixed, and use Lemma 13 bound $|\mathcal{A}_x \setminus C|$ from above and Lemma 12 to bound $|\mathcal{A} \setminus C|$ from below.

Thus we obtain the following upper bound:

$$\frac{|\mathcal{A}_x \setminus C|}{|\mathcal{A} \setminus C|} \leq \frac{[\dot{\alpha}]_{q,\delta} - [\ddot{\alpha}]_{q,\delta}}{[\dot{\alpha}]_{q,\delta}(q^{\delta - \alpha} - c)}.$$

Once again we may use Lemma 5.2 and some algebra to obtain

$$\frac{P(x \in A | C, \mathcal{A})}{P(x \in A | C)} \leq \frac{q^{2\delta} - cq^\delta - q^{\delta + \alpha} + cq^\alpha}{q^{2\delta} - cq^{\delta + \alpha} - q^\delta + cq^\alpha}. \qquad \square$$

Example 1. *Let $q = 2^{14}$, $\alpha = 1$ and $\delta = 3$. This gives rise to the triple*

$$a = 16{,}384$$
$$b = 4{,}398{,}046{,}494{,}716$$
$$c = 4.$$

Although the number of cards is rather large, this triple is remarkable in that it may be considered floating-point perfectly secure; *indeed, by Lemma 14 the geometric strategy is 1.118×10^{-8}-strongly safe for this choice of parameters.*

In fact, when q is large, some simpler bounds will suffice for our purposes.

Corollary 3. *If $\mathcal{A}$ is an announcement of the geometric strategy with parameters α, δ and $C \in \binom{\Omega}{c}$ is non-empty, then*

$$1 - \frac{cq^{\alpha}}{q^{\delta} - 1} \leq \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} \tag{6}$$

and

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} \leq 1 + \frac{c(q^{\delta} + 1) + q^{\delta - \alpha}}{q^{2\delta - \alpha} - cq^{\delta} - q^{\delta - \alpha}}. \tag{7}$$

Proof. Observe that, since $\delta \geq 2$, it follows that $-q^{\delta + \alpha} + q^{\alpha} < 0$; thus we can remove this term from the denominator in (4), as well as some positive terms from the numerator to obtain

$$\frac{q^{2\delta} - cq^{\delta + \alpha} - q^{\delta}}{q^{2\delta} - q^{\delta}} \leq \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)},$$

which gives us our lower bound (6) by simplifying.

We may also obtain a simpler upper bound by removing negative terms from the numerator and positive terms from the denominator, giving us

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} \leq \frac{q^{2\delta} + cq^{\alpha}}{q^{2\delta} - cq^{\delta + \alpha} - q^{\delta}},$$

which factoring q^{α} and performing polynomial division becomes our simplified upper bound (7). □

6.3 Convergence

Our simplified bounds from Corollary 3 will be enough to yield many tuples for which the geometric strategy is ε-strongly safe for arbitrarily small ε. It is based on the following.

Theorem 3. *Let $\varepsilon > 0$, $1 \leq \alpha < \delta$ and $\bar{c} \colon \mathbb{N} \to \mathbb{N}$ be such that $\bar{c}(q) = o(q^{\delta - \alpha})$. Then, if q is a large enough prime power, the geometric strategy with parameters q, α, δ is ε-strongly safe for any $c < \bar{c}(q)$.*

Proof. If $\bar{c}(q) = o(q^{\delta - \alpha})$ then $1 - \frac{\bar{c}(q)q^{\alpha}}{q^{\delta} - 1}$ and $1 + \frac{\bar{c}(q)(q^{\delta} + 1) + q^{\delta - \alpha}}{q^{2\delta - \alpha} - \bar{c}(q)q^{\delta} - q^{\delta - \alpha}}$ both converge to 1 as $q \to \infty$. It follows from Corollary 3 that if q is large and $c < \bar{c}(q)$,

$$\left| \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} - 1 \right| < \varepsilon,$$

which means that the geometric strategy is ε-strongly safe. □

However, convergence may be quicker or slower depending on how we choose $\bar{c}$. For example, if we fix $\xi > 0$ and take $\bar{c}(q) = \lfloor q^{\delta - \alpha - \xi} \rfloor$, then this quotient will tend to one, but if ξ is very small we may need a very large number of cards for it to be less than some given ε. More generally, we have the following:

17

Theorem 4. *Fix $1 \leq \alpha < \delta$, $\xi \in (0, \delta - \alpha)$ and $\bar{c} \colon \mathbb{N} \to \mathbb{N}$ with $\bar{c}(q) \leq q^{\delta - \alpha - \xi}$. Then, for q a prime power, any announcement $\mathcal{A}$ of the geometric strategy any card x and any set of C cards with at most $\bar{c}(q)$ elements,*

$$\frac{P(x \in A | C, \mathcal{A})}{P(x \in A | C)} = 1 + O(1/q^\xi).$$

Proof. If we take $c = \bar{c}(q) \leq q^{\delta - \alpha - \xi}$, we have that

$$\frac{cq^\alpha}{q^\delta - 1} \leq \frac{q^{\delta - \xi}}{q^\delta - 1} = O(1/q^\xi),$$

whereas

$$\frac{c(q^\delta + 1) + q^{\delta - \alpha}}{q^{2\delta - \alpha} - cq^\delta - q^{\delta - \alpha}} \leq \frac{q^{2\delta - \alpha - \xi} + q^{\delta - \alpha - \xi} + q^{\delta - \alpha}}{q^{2\delta - \alpha} - q^{2\delta - \alpha - \xi} - q^{\delta - \alpha}} = O(1/q^\xi).$$

The theorem then follows from Corollary 3. □

Here we see a trade-off between keeping Cath's hand relatively large and obtaining a good rate of convergence for our bounds. Observe, however, that the larger c is, the less tight our bounds are, so despite our bounds converging rather slowly there may be smaller examples with a large degree of security.

7 Choosing good parameters

In this section we will focus on strategies for finding specific choices of parameters for which the geometric protocol is ε-safe. In particular, we will fix $\varepsilon = 0.05$, and use our bounds to find several explicit tuples for which the geometric strategy is ε-safe. It is interesting to compare this to [11], where many choices of parameters for which the protocol is perfectly safe are exhibited. All of the tuples presented there have $c \leq 3$, and the authors discuss the difficulty of finding perfectly safe strategies for larger c. As we shall see this becomes substantially simpler if we weaken our requirements to (e.g.) 0.05-strong safety. Thus we may argue that passing to a weaker notion of security allows us to make the Russian cards problem substantially easier to solve without compromising security in a practically meaningful way.

7.1 Cath has one card

The notion of perfect security for the Russian cards problem was introduced in [12], where several examples with $c = 1$ are provided. Here we will show that, in this setting, the bounds we have found may also be used to establish perfect security in the case of the geometric strategy.

Corollary 4. *Given $1 \leq \alpha < \delta$ and a prime power q, the geometric strategy is perfectly safe for $(a, b, 1)$ with $a = q^\alpha$ and $b = q^\delta - a - 1$.*

Proof. We will use our original bounds from Lemma 14. Setting $c = 1$ in (4) we see that

$$\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} \leq \frac{q^{2\delta} - q^\delta - q^{\delta+\alpha} + q^\alpha}{q^{2\delta} - q^{\delta+\alpha} - q^\delta + q^\alpha} = 1.$$

Similarly, we substitute $c = 1$ in (5) to obtain

$$1 = \frac{q^{2\delta} - q^{\delta+\alpha} - q^\delta + q^\alpha - 1 + 1}{q^{2\delta} - q^\delta - q^{\delta+\alpha} + q^\alpha} \leq \frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)}.$$

Thus we have seen that $\frac{P(x \in A|C, \mathcal{A})}{P(x \in A|C)} = 1$, that is, $P(x \in A|C, \mathcal{A}) = P(x \in A|C)$. $\qquad\square$

Hence our bounds give an alternative proof that the geometric strategy is perfectly secure when $c = 1$. Now let us turn our attention to larger c.

7.2 Making Cath's hand large

Suppose that we wish to obtain good tuples for which c is as large as possible relative to Alice's hand. Cath's hand is bounded by two expressions on α, one increasing on α ($c < q^\alpha - q^{\alpha-1}$) and one decreasing ($c = o(q^{\delta-\alpha})$). Thus, the maximum value that c may take is when the two bounds coincide, which occurs approximately when $\delta = 2\alpha$ or $\delta = 2\alpha + 1$.

The latter case is interesting, since we already have that $q^\alpha - q^{\alpha-1} < q^{\delta-\alpha-1}$. Thus in cases that Alice holds relatively few cards, less than the square root of the deck, our informativity bound will already give us ε-strong safety for large values of q. To be precise, we have the following:

Corollary 5. *Let $\varepsilon, \beta > 0$ and $\gamma \in (0,1)$. Then, there are infinitely many values of a such that for any $c < \gamma a$ there is $b < a^{2+\beta}$ so that the geometric strategy is informative and ε-strongly safe for (a, b, c).*

Proof. Let $\varepsilon, \beta > 0$ and $\gamma \in (0,1)$. Pick α large enough so that $1/\alpha \leq \beta$ and Q large enough so that $1/Q < (1-\gamma)/2$. Set $\delta = 2\alpha + 1$ and $\bar{c}(q) = q^\alpha + q^{\alpha-1} - 1$. Then, since $\delta - \alpha = \alpha + 1$ we have that $\bar{c}(q) = o(q^{\delta-\alpha})$, from which it follows from Theorem 3 that for large q, the geometric strategy is informative and ε-strongly safe for $a = q^\alpha$, $c \leq \bar{c}(q)$ and $b = q^\delta - a - c$. In particular we may also take $q > Q$, so that

$$\bar{c}(q) = q^\alpha - q^{\alpha-1} - 1 = (1 - 1/q - 1/q^\alpha)a > \gamma a.$$

Meanwhile, $b < q^\delta = (q^\alpha)^{\frac{2\alpha+1}{\alpha}} < a^{2+\beta}$, so all desired conditions are met. $\qquad\square$

Compare the above result to Corollary 1. As before we can have $c = O(a)$, but this time instead of having $b < ac$ we must take $b = O(ac^{1+\beta})$. Thus the price of obtaining ε-strong security is to make Bob's hand a bit larger than we would need for weak security. In Figure 4, we fix values of γ and β and use the strategy of Corollary 5 and its proof to find tuples for which the protocol is 0.5-strongly secure.

a	b	c	q	α	γ	Lower	Upper
8	500	4	2^3	1	0.5	0.9527	1.0438
9	715	5	3^3	1	0.5	0.9503	1.0468
11	1,316	4	11	1	0.3	0.9750	1.0233
13	2,180	4	13	1	0.3	0.9821	1.0167
17	4,881	15	17	1	0.8	0.9515	1.0480
19	6,836	4	19	1	0.2	0.9916	1.0079
49	16,743	15	7	2	0.3	0.9591	1.0418
125	77,974	26	5	3	0.2	0.9599	1.0414

Figure 4: Tuples for which the geometric strategy is 0.5-strongly secure with q a prime power, $a = q^\alpha$, $c \geq \gamma\alpha$, and $b = q^{2\alpha+1} - a - c$.

7.3 Making Bob's hand small

We may also give a ε-strongly secure analogue of Corollary 2. Suppose that we instead want to have a small number of cards in Bob's hand relative to Alice's. In our above construction Bob's hand grew relatively quickly, so we want a different strategy for selecting parameters. The trade-off will be that Cath's hand may be substantially smaller than Alice's. In general if we want Bob to have less than $a^{1+\beta}$ cards, then Cath must have less than a^γ for some $\gamma < \beta$.

Corollary 6. *Let $\varepsilon > 0$, $\gamma \in (0,1)$ and $\beta > \gamma$ be such that $\beta \in \mathbb{Q}$. Then, there are infinitely many values of a such that for any $c < a^\gamma$ there is $b < a^{1+\beta}$ such that the geometric strategy is informative and ε-strongly safe for (a, b, c).*

Proof. Similar to the proof of Corollary 2, but taking $c < q^{\gamma\alpha}$ and using Theorem 3. □

Once again, we may obtain ε-strong security for infinitely many tuples (a, b, c) where $c < a$ and $b = O(ac^{1+\beta})$. So the takeaway in either case is that, making Bob's hand only a bit bigger compared to the rest of the deck and choosing an appropriately large deck, we may obtain ε-strong security instead of merely weak security. In Figure 5 we use this idea to find additional tuples for which the geometric protocol is 0.5-safe.

8 Concluding remarks

While the Russian cards provides a setting in which we may attain unconditionally safe communication, many known solutions to the Russian cards problem are only weakly safe, meaning that they may provide the eavesdropper with probabilistic information. Although perfectly secure solutions are known, it is somewhat difficult to find tuples for which this level of security may be attained. In this paper we have shown, however, that the amount of probabilistic information obtained by the eavesdropper may be controlled, to the extent that in

a	b	c	q	α	γ	δ	Lower	Upper
16	1,004	4	4	2	0.5	5	0.9525	1.0470
25	3,095	5	5	2	0.5	5	0.9677	1.0321
27	6,524	10	3	3	0.7	8	0.9628	1.0373
107	11,336	6	107	1	0.4	2	0.9528	1.0490
529	11,636	2	23	2	0.15	3	0.9545	1.0475
529	279,289	23	23	2	0.5	4	0.9583	1.0433
11,449	1,213,588	6	107	2	0.2	3	0.9528	1.0495
6,561	4,776,375	33	9	4	0.4	7	0.9560	1.0459

Figure 5: Tuples for which the geometric strategy is 0.05-strongly secure with q a prime power, $\delta \geq \alpha > 0$, $\gamma < \delta/\alpha - 1$, $a = q^\alpha$, $c = \lfloor a^\gamma \rfloor$, and $b = q^\delta - a - c$.

some cases we can obtain a degree of safety indistinguishable from perfect safety for all practical purposes. Weakening the notion of perfect security has led to an infinite number of new tuples for which we may still obtain a high degree of security, and indeed the bounds we have given may be used to analyze the level of security in any instance of the geometric strategy. Moreover, our techniques had the added bonus of replicating some results of [12].

There are further directions that may be explored. Although our bounds are tight when $c = 1$, the larger c is, the less exact they are, which may keep us from identifying many tuples for which we have a high degree of security. These bounds may be improved with a deeper (and, possibly, messier) combinatorial analysis which takes into account collinear points using the inclusion-exclusion principle. In fact, tailor-made bounds can be used for specific values of c that may be of interest.

Finally, this analysis could be generalized further to include other combinatorial constructions, for example considering a wider class of designs. Such efforts could very well lead to more flexible methods of finding tuples for which there are strategies with very high levels of security.

References

[1] M. Albert, R. Aldred, M. Atkinson, H. van Ditmarsch, and C. Handley. Safe communication for card players by combinatorial designs for two-step protocols. *Australasian Journal of Combinatorics*, 33:33–46, 2005.

[2] A. Cordón-Franco, H. van Ditmarsch, D. F. Duque, and F. Soler-Toscano. A geometric protocol for cryptography with cards. *Designs, Codes and Cryptography*, 74(1):113–125, 2015.

[3] A. Cordón-Franco, H. van Ditmarsch, D. Fernández-Duque, J. Joosten, and F. Soler-Toscano. A secure additive protocol for card players. *Australasian Journal of Combinatorics*, 54:163–176, 2012.

[4] A. Cordón-Franco, H. van Ditmarsch, D. Fernández-Duque, and F. Soler-Toscano. A colouring protocol for the generalized Russian cards problem. *Theoretical Computer Science*, 495:81–95, 2013.

[5] P. Dembowski. *Finite Geometries (reprint)*. Springer, 1997.

[6] Z. Duan and C. Yang. Unconditional secure communication: a Russian cards protocol. *Journal of Combinatorial Optimization*, 19:501–530, 2010.

[7] D. Fernández-Duque and V. Goranko. Secure aggregation of distributed information. *CoRR*, abs/1407.7582, 2014.

[8] T. P. Kirkman. On a problem in combinations. *Cambridge and Dublin Mathematical Journal*, 2:191–204, 1847.

[9] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.

[10] D. R. Stinson. *Cryptography: theory and practice*. CRC press, 2005.

[11] C. M. Swanson and D. R. Stinson. Additional constructions to solve the generalized russian cards problem using combinatorial designs. *arXiv preprint arXiv:1401.1526*, 2014.

[12] C. M. Swanson and D. R. Stinson. Combinatorial solutions providing improved security for the generalized russian cards problem. *Designs, Codes and Cryptography*, 72(2):345–367, 2014.

[13] H. van Ditmarsch. The Russian cards problem. *Studia Logica*, 75:31–62, 2003.

[14] H. van Ditmarsch and F. Soler-Toscano. Three steps. In *Proc. of CLIMA XII*, LNCS 6814, pages 41–57. Springer, 2011.